Posudek bakalářské práce

předložené na Matematicko-fyzikální fakultě
Univerzity Karlovy v Praze

X posudek oponenta

Autor/ka: Szabolcs Gróf

Název práce: STalk - zabezpečená aplikace pro komunikaci

Studijní program a obor: programování [IP]

Rok odevzdání: **2007**

Jméno a tituly vedoucího/oponenta: **Dan Lukeš**

Pracoviště: **SISAL**

	excelentní	**odpovídající**	**slabší**	**nevyhovující**
Náročnost zadaného tématu	X			
Míra splnění zadání		X		
Struktura textové části práce		X		
Jazyková a typografická úroveň		X		
Analýza		X		
Vývojová dokumentace		X		
Uživatelská dokumentace	X			
Kvalita zpracování softwarové části			X	
Stabilita aplikace			X	

Nejvýznamnější klady:
Funguje (což u implementace sifrováni neni tak málo)

Nejzávažnější nedostatky:
Programátorsky poměrně špatný kód (nekontroluje zda volání externích funkcí dopadio úspěšně; užívání nereentrantních funkci pri obsluze asynchronních signálu; ...)

Některé znalosti popsané v teoretické části práce se nepromítly do implementace (generátor DES klíču vrátí i weak/semiweak klíče; smyčka čtení dat ze sítě obsahuje přesně tu chybu před kterou teoretická část explicitně varuje)

Další poznámky:

Nevyhovující kvalitu kódu vyváží fakt, že pro vlastní implementaci DES, RSA a podpurných subsystemů (generátor prvočísel) bylo nutné nastudovat poměrně složitou teorii, což je celá polovina zadání. Práce by rozhodně měla být obhájena.

	výborně	velmi dobře	dobře	neprospěl/a
Návrh známky		X		

Datum: 4. IX 2007

Podpis: **Dan Lukeš**